



## **Failure Modes, Effects and Diagnostic Analysis**

Project:  
9203 Solenoid / Alarm Driver

Customer:  
PR electronics A/S  
Rønde  
Denmark

Contract No.: PR electronics 06/03-19  
Report No.: PR electronics 06/03-19 R023  
Version V1, Revision R2; September 2010  
Stephan Aschenbrenner, Alexander Dimov



## Management summary

This report summarizes the results of the hardware assessment carried out on the 9203 Solenoid / Alarm Driver with product version 9203-001.

There are two variants of the 9203 Solenoid / Alarm Driver; the 9203 B1A/B low current type (single or dual channel) and the 9203 B2A high current type (single channel).

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) is calculated for the devices. For full assessment purposes all requirements of IEC 61508 must be considered.

For safety applications only the described versions are considered. All other possible output variants or electronics are not covered by this report.

The failure rates used in this analysis are from the *exida* Electrical & Mechanical Component Reliability Handbook for Profile 1<sup>1</sup>. The analysis was carried out with the basic failure rates from the Siemens standard SN 29500. However as the comparison between these two databases has shown that the differences are within an acceptable tolerance the failure rates of the *exida* database are listed.

The two channels on the two channel devices shall not be used in the same safety function, e.g. to increase the hardware fault tolerance to achieve a higher SIL, as they contain common components. The FMEDA applies to either channel used in a single safety function. The two channels may be used in separate safety functions if due regard is taken of the possibility of common failures.

The 9203 Solenoid / Alarm Driver is considered to be a Type B<sup>2</sup> subsystem with a hardware fault tolerance of 0. For Type B subsystems with a hardware fault tolerance of 0 the SFF has to be  $\geq 90\%$  for SIL 2 subsystems according to table 2 of IEC 61508-2.

It is important to realize that the “no effect” failures and the “annunciation” failures are included in the “safe” failure category according to IEC 61508. Note that these failures on its own will not affect system reliability or safety, and should not be included in spurious trip calculations.

A user of the 9203 Solenoid / Alarm Driver can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in sections 4.3.1 and 4.3.2 along with all assumptions.

---

<sup>1</sup> For details see Appendix 3.

<sup>2</sup> Type B subsystem: “Complex” subsystem (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

**Table 1: Summary for the 9203 Solenoid / Alarm Driver (low current type) - IEC 61508 failure rates**

	<i>exida</i> Profile 1
<b>Fail Safe Detected (<math>\lambda_{SD}</math>)</b>	<b>0</b>
Fail safe detected	0
<b>Fail Safe Undetected (<math>\lambda_{SU}</math>)</b>	<b>477</b>
Fail safe undetected	170
Fail detected (detected by internal diagnostics)	62
No effect	171
Annunciation detected	72
Annunciation undetected (95%)	2
<b>Fail Dangerous Undetected (<math>\lambda_{DU}</math>)</b>	<b>43<sup>3</sup></b>
Fail dangerous undetected	43
Annunciation undetected (5%)	0
No part	128
<b>Total failure rate (safety function)</b>	<b>520 FIT</b>
<b>SFF<sup>4</sup></b>	<b>91.7%</b>
<b>MTBF</b>	<b>176 years</b>
<b>SIL AC<sup>5</sup></b>	<b>SIL2</b>

The failure rates are valid for the useful life of the 9203 Solenoid / Alarm Driver (see Appendix 2).

<sup>3</sup> This value corresponds to a PFH of 4.30E-08 1/h considering a fault reaction time of 1 minute.

<sup>4</sup> The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>5</sup> SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled.

**Table 2 Summary for the 9203 Solenoid / Alarm Driver (high current type) - IEC 61508 failure rates**

	<i>exida</i> Profile 1
<b>Fail Safe Detected (<math>\lambda_{SD}</math>)</b>	<b>0</b>
Fail safe detected	0
<b>Fail Safe Undetected (<math>\lambda_{SU}</math>)</b>	<b>480</b>
Fail safe undetected	170
Fail detected (detected by internal diagnostics)	62
No effect	174
Annunciation detected	72
Annunciation undetected (95%)	2
<b>Fail Dangerous Undetected (<math>\lambda_{DU}</math>)</b>	<b>46<sup>6</sup></b>
Fail dangerous undetected	46
Annunciation undetected (5%)	0
No part	128
<b>Total failure rate (safety function)</b>	<b>526 FIT</b>
<b>SFF<sup>7</sup></b>	<b>91.2%</b>
<b>MTBF</b>	<b>175 years</b>
<b>SIL AC<sup>8</sup></b>	<b>SIL2</b>

The failure rates are valid for the useful life of the 9203 Solenoid / Alarm Driver (see Appendix 2).

<sup>6</sup> This value corresponds to a PFH of 4.60E-08 1/h considering a fault reaction time of 1 minute.

<sup>7</sup> The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>8</sup> SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled.



## Table of Contents

Management summary .....	2
1 Purpose and Scope .....	6
2 Project management.....	7
2.1 <i>exida</i> .....	7
2.2 Roles and parties .....	7
2.3 Standards / Literature used.....	7
2.4 Reference documents.....	7
2.4.1 Documentation provided by the customer.....	7
2.4.2 Documentation generated by <i>exida</i> .....	7
3 Description of the analyzed subsystems.....	8
4 Failure Modes, Effects, and Diagnostic Analysis .....	9
4.1 Description of the failure categories.....	9
4.2 Methodology – FMEDA, Failure rates.....	10
4.2.1 FMEDA.....	10
4.2.2 Failure rates .....	10
4.2.3 Assumptions.....	11
4.3 Results.....	11
4.3.1 9203 Solenoid / Alarm Driver (low current type) .....	12
4.3.2 9203 Solenoid / Alarm Driver (high current type).....	13
5 Using the FMEDA results.....	14
5.1 Example PFD <sub>AVG</sub> calculation .....	14
6 Terms and Definitions .....	15
7 Status of the document.....	16
7.1 Liability.....	16
7.2 Releases.....	16
Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test ..	17
Appendix 1.1: Possible proof tests to detect dangerous undetected faults.....	18
Appendix 2: Impact of lifetime of critical components on the failure rate .....	19
Appendix 3: Description of the considered profiles.....	20
<i>exida</i> electronic database: .....	20

## 1 Purpose and Scope

Generally three options exist when doing an assessment of sensors, interfaces and/or final elements.

### Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or ISO 13849-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand ( $PFD_{AVG}$ ). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. This option does not include an assessment of the development process.

### Option 2: Hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511

Option 2 extends Option 1 with an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. When combined with plant specific proven-in-use records, it may help with prior-use justification per IEC 61511 for sensors, final elements and other PE field devices.

### Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or ISO 13849-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

### **This assessment shall be done according to option 3.**

This document shall describe the results of the FMEDA carried out on the 9203 Solenoid / Alarm Driver with product version 9203-001. The FMEDA is part of a full functional safety assessment according to IEC 61508.

The information in this report can be used to evaluate whether a final element subsystem, including the 9203 Solenoid / Alarm Driver meets the average Probability of Failure on Demand ( $PFD_{AVG}$ ) / Probability of dangerous Failure per Hour (PFH) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508. It **does not** consider any calculations necessary for proving intrinsic safety.



## 2 Project management

### 2.1 *exida*

*exida* is one of the world's leading knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a partnership company with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detail product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

### 2.2 Roles and parties

PR electronics A/S  <i>exida</i>	Manufacturer of the 9203 Solenoid / Alarm Driver.  Performed the hardware assessment and reviewed the FMEDA provided by the customer.
--	---

PR electronics A/S contracted *exida* in October 2008 with the review of the FMEDA and PFD<sub>AVG</sub> calculation of the above mentioned device.

### 2.3 Standards / Literature used

The services delivered by *exida* were performed based on the following standards / literature.

[N1]	IEC 61508-2:2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	EMCRH, 2nd Edition, 2008	<i>exida</i> L.L.C, Electrical & Mechanical Component Reliability Handbook, Second Edition, 2008, ISBN 978-0-9727234-6-6

### 2.4 Reference documents

#### 2.4.1 Documentation provided by the customer

[D1]	9203-1-V6R0.pdf of 13.01.2010	Schematic drawings, No. 9203-1-V6R0 (page SH1 to SH7) of 12.01.2010
[D2]	Feedback_on_Review.txt of 28.01.09	Feedback on FMEDA review comments
[D3]	9203 FMEDA high current V6R0.xls of 13.01.2010	FMEDA results file generated by customer
[D4]	9203 FMEDA low current V6R0.xls of 13.01.2010	FMEDA results file generated by customer
[D5]	9203 Safety Manual V1R0.pdf	Safety Manual "9203 Solenoid / Alarm Driver" V1R0

#### 2.4.2 Documentation generated by *exida*

[R1]	9203 FMEDA high current V4R0 - Review SA.xls of 15.12.2008	FMEDA review comments
[R2]	9203 FMEDA low current V4R0 - Review SA.xls of 15.12.2008	FMEDA review comments

### 3 Description of the analyzed subsystems

The 9203 Solenoid / Alarm Driver series (see block diagram Figure 1) feature an intrinsically safe output with limited current and voltage, thus making direct connection to loads in the Ex-area possible. Typical applications are the control of alarms or solenoids / valves. The loads can be controlled when the corresponding input pins of X10 are short circuit, switched from external voltage  $> +12$  VDC and  $< +31.2$  VDC, or switched by an PNP from external supply, or switched to ground by NPN transistor. If the input pins are left open, the outputs are de-energized. There are two main types of the 9203 Solenoid / Alarm Driver; the 9203 B1/A or B (single or dual channel) as the low current type with 93/100/110mA outgoing current, and the 9203 B2A (single channel) high current type with 115/125/135mA outgoing current. The different currents are found on the three connector poles of each channel output connector X40/X50. The outgoing voltage is limited to 28 VDC.

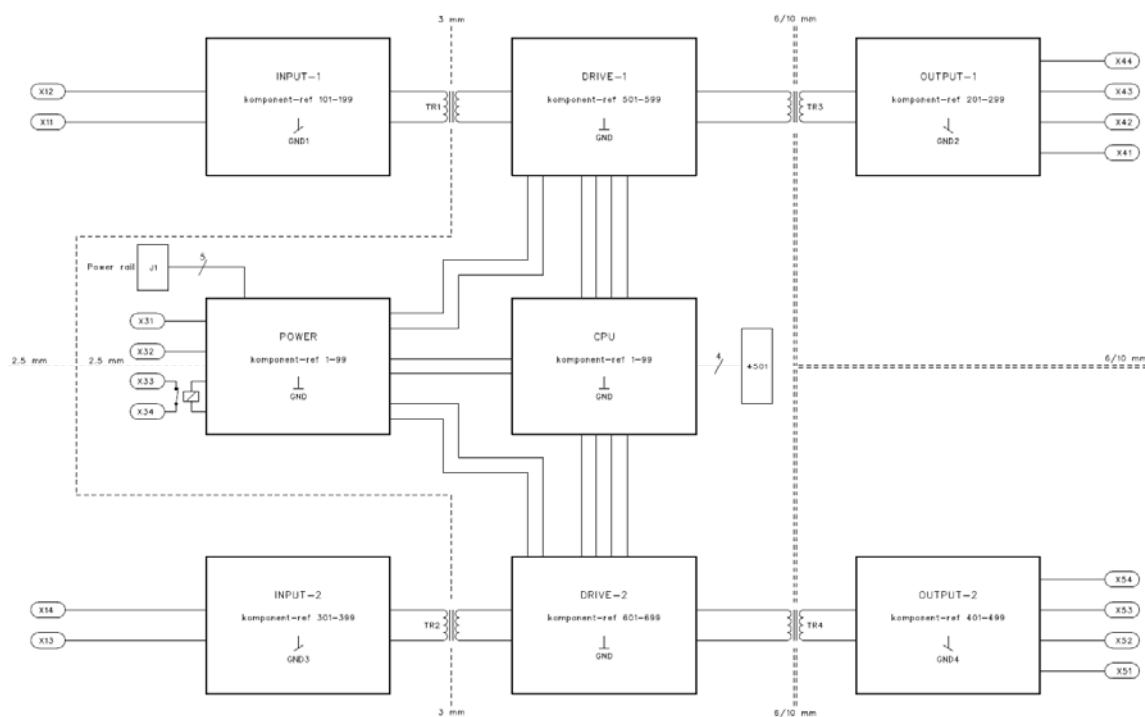


Figure 1: Block diagram of the 9203 Solenoid / Alarm Driver series

## 4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was prepared by PR electronics A/S and reviewed by *exida*. The results are documented in [D3] and [D4]. Failures are classified according to the following failure categories.

### 4.1 Description of the failure categories

In order to judge the failure behavior of the 9203 Solenoid / Alarm Driver, the following definitions for the failure of the product were considered.

Fail-Safe State	The fail-safe state is defined as the output being de-energized.
Fail Safe	Failure that causes the subsystem to go to the defined fail-safe state without a demand from the process.
Fail Dangerous	A dangerous failure (D) is defined as a failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state)
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by internal diagnostics.
Fail Dangerous Detected	Failure that is dangerous but is detected by internal diagnostics and causes the output signal to go to the fail-safe state.
No Effect	Failure mode of a component that plays a part in implementing the safety function but is neither a safe failure nor a dangerous failure. For the calculation of the SFF it is treated like a safe undetected failure.
Annunciation	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit). Annunciation failures are divided into annunciation detected (AD) and annunciation undetected (AU) failures. For the calculation of the SFF they are treated to 5% as a "Dangerous Undetected" failure and to 95% as a "No Effect" failure.
No Part	Component that plays no part in implementing the safety function but is part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account. It is also not part of the total failure rate.

The failure categories listed above expand on the categories listed in IEC 61508 which are only safe and dangerous, both detected and undetected. The reason for this is that not all failure modes have effects that can be accurately classified according to the failure categories listed in IEC 61508:2000.

The "No Effect" and "Annunciation Undetected" failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508. In IEC 61508.2000 the "No Effect" failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.

## 4.2 Methodology – FMEDA, Failure rates

### 4.2.1 FMEDA

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system under consideration.

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extensions to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

### 4.2.2 Failure rates

The failure rate data used by *exida* in this FMEDA are from the *exida* Electrical & Mechanical Component Reliability Handbook for Profile 1. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment similar to *exida* Profile 1. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

For hardware assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events however should be considered as random failures. Examples of such failures are loss of power or physical abuse.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its “useful life”.

The user of these numbers is responsible for determining their applicability to any particular environment. Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system that indicates higher failure rates, the higher numbers shall be used. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

### 4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the 9203 Solenoid / Alarm Driver.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The device is installed per manufacturer's instructions.
- Failures during parameterization are not considered.
- Sufficient tests are performed prior to shipment to verify the absence of vendor and/or manufacturing defects that prevent proper operation of specified functionality to product specifications or cause operation different from the design analyzed.
- The Mean Time To Restoration (MTTR) after a safe failure is 24 hours.
- External power supply failure rates are not included.
- Only the described versions are used for safety applications.
- Only one input and one output are part of the considered safety function.
- The worst-case internal fault detection time is 1 minute.

### 4.3 Results

For the calculation of the Safe Failure Fraction (SFF) and  $\lambda_{total}$  the following has to be noted:

$$\lambda_{total} = \lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}$$

$$SFF = 1 - \lambda_{DU} / \lambda_{total}$$

$$DC_D = \lambda_{DD} / (\lambda_{DD} + \lambda_{DU})$$

$$MTBF = MTTF + MTTR = (1 / (\lambda_{total} + \lambda_{no\ part})) + 24\ h$$

#### 4.3.1 9203 Solenoid / Alarm Driver (low current type)

The FMEDA carried out on 9203 Solenoid / Alarm Driver (low current type) leads under the assumptions described in section 4.2.3 to the following failure rates:

	<i>exida</i> Profile 1
<b>Fail Safe Detected (<math>\lambda_{SD}</math>)</b>	<b>0</b>
Fail safe detected	0
<b>Fail Safe Undetected (<math>\lambda_{SU}</math>)</b>	<b>477</b>
Fail safe undetected	170
Fail detected (detected by internal diagnostics)	62
No effect	171
Annunciation detected	72
Annunciation undetected (95%)	2
<b>Fail Dangerous Undetected (<math>\lambda_{DU}</math>)</b>	<b>43<sup>9</sup></b>
Fail dangerous undetected	43
Annunciation undetected (5%)	0
No part	128
<b>Total failure rate (safety function)</b>	<b>520 FIT</b>
<b>SFF<sup>10</sup></b>	<b>91.7%</b>
<b>MTBF</b>	<b>176 years</b>
<b>SIL AC<sup>11</sup></b>	<b>SIL2</b>

<sup>9</sup> This value corresponds to a PFH of 4.30E-08 1/h considering a fault reaction time of 1 minute.

<sup>10</sup> The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>11</sup> SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled.

#### 4.3.2 9203 Solenoid / Alarm Driver (high current type)

The FMEDA carried out on 9203 Solenoid / Alarm Driver (high current type) leads under the assumptions described in section 4.2.3 to the following failure rates:

	<i>exida</i> Profile 1
<b>Fail Safe Detected (<math>\lambda_{SD}</math>)</b>	<b>0</b>
Fail safe detected	0
<b>Fail Safe Undetected (<math>\lambda_{SU}</math>)</b>	<b>480</b>
Fail safe undetected	170
Fail detected (detected by internal diagnostics)	62
No effect	174
Annunciation detected	72
Annunciation undetected (95%)	2
<b>Fail Dangerous Undetected (<math>\lambda_{DU}</math>)</b>	<b>46<sup>12</sup></b>
Fail dangerous undetected	46
Annunciation undetected (5%)	0
No part	128
<b>Total failure rate (safety function)</b>	<b>526 FIT</b>
<b>SFF<sup>13</sup></b>	<b>91.2%</b>
<b>MTBF</b>	<b>175 years</b>
<b>SIL AC<sup>14</sup></b>	<b>SIL2</b>

<sup>12</sup> This value corresponds to a PFH of 4.60E-08 1/h considering a fault reaction time of 1 minute.

<sup>13</sup> The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>14</sup> SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled.

## 5 Using the FMEDA results

The following section describes how to apply the results of the FMEDA.

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire SIF. *exida* recommends the accurate Markov based exSILentia tool for this purpose.

The following results must be considered in combination with  $PFD_{AVG}$  values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL).

### 5.1 Example $PFD_{AVG}$ calculation

An average Probability of Failure on Demand ( $PFD_{AVG}$ ) calculation is performed for a single channel (1oo1) 9203 Solenoid / Alarm Driver including both low and high current type considering a proof test coverage of 95% (see Appendix 1.1) and a mission time of 10 years. The failure rate data used in this calculation is displayed in section 4.3.1 and 4.3.2. The resulting  $PFD_{AVG}$  values for a variety of proof test intervals are displayed in Table 3.

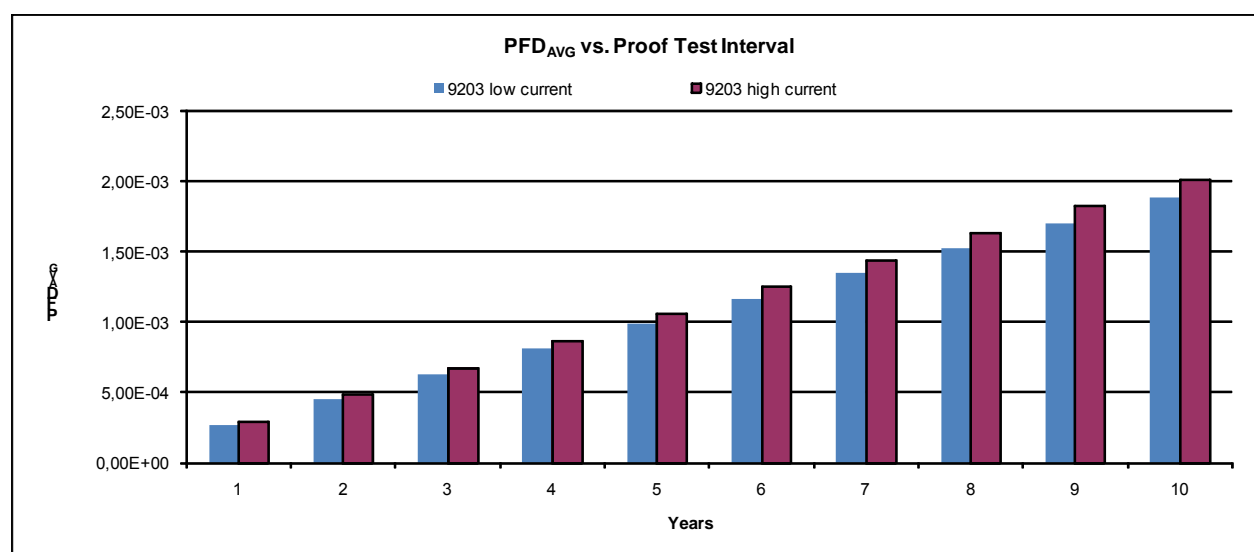
For SIL2 applications, the  $PFD_{AVG}$  value needs to be  $< 1.00E-02$ .

**Table 3:  $PFD_{AVG}$  values - 9203 Solenoid / Alarm Driver**

Type	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
9203 Solenoid / Alarm Driver, Low current	$PFD_{AVG} = 2.73E-04$	$PFD_{AVG} = 4.52E-04$	$PFD_{AVG} = 9.89E-04$
9203 Solenoid / Alarm Driver, High current	$PFD_{AVG} = 2.92E-04$	$PFD_{AVG} = 4.84E-04$	$PFD_{AVG} = 1.06E-03$

This means that for a SIL2 application, the  $PFD_{AVG}$  for a 1-year Proof Test Interval is approximately equal to 3% of the allowed range.

Figure 2 shows the time dependent curve of  $PFD_{AVG}$ .



**Figure 2:  $PFD_{AVG}(t)$  - 9203 Solenoid / Alarm Driver**

## 6 Terms and Definitions

FIT	Failure In Time ( $1 \times 10^{-9}$ failures per hour)
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency.
High demand mode	Mode, where the frequency of demands for operation made on a safety-related system is greater than twice the proof check frequency.
MTTR	Mean Time To Restoration
$PFD_{AVG}$	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
Type B subsystem	“Complex” subsystem (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2
T[Proof]	Proof Test Interval



## 7 Status of the document

### 7.1 Liability

*exida* prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market place, *exida* is actively involved in evolving best practices prior to official release of updated standards so that our reports effectively anticipate any known changes. In addition, most changes are anticipated to be incremental in nature and results reported within the previous three year period should be sufficient for current usage without significant question.

Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years and the exact results are critical to the SIL verification you may wish to contact the product vendor to verify the current validity of the results.

### 7.2 Releases

Version History: V1R2: Purpose and Scope section modified; September 27, 2010

V1R1: Description of proof test modified; March 9, 2010

V1R0: Review comments incorporated; January 15, 2010

V0R1: Initial version; November 26, 2009

Authors: Stephan Aschenbrenner, Alexander Dimov

Review: V0R1: Hans Jørgen Eriksen (PR electronics A/S); November 30, 2009

Rachel Amkreutz (*exida*); January 12, 2010

Release status: Released to PR electronics A/S as part of a complete functional safety assessment according to IEC 61508.

## Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test

According to section 7.4.3.2.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests.

This means that it is necessary to specify how dangerous undetected faults which have been noted during the FMEDA can be detected during proof testing.

Tables 5/6 show an importance analysis of the dangerous undetected faults and indicates how these faults can be detected during proof testing.

Appendix 1 shall be considered when writing the safety manual as it contains important safety related information.

**Table 4: Importance analysis of dangerous undetected faults (low current type)**

Component	% of total $\lambda_{du}$	Detection through
Z202, Z203 Z204, Z205 Z206, Z207	7,76%	100% functional test with different expected output signals
T505	7,05%	100% functional test with different expected output signals
T503-B	5,88%	100% functional test with different expected output signals
T202	5,88%	100% functional test with different expected output signals
IC501-B	5,64%	100% functional test with different expected output signals
C105, C106	4,70%	100% functional test with different expected output signals
T201	3,88%	100% functional test with different expected output signals
D102	3,76%	100% functional test with different expected output signals
C201	3,76%	100% functional test with different expected output signals
T503-A	3,53%	100% functional test with different expected output signals

**Table 5: Importance analysis of dangerous undetected faults (high current type)**

Component	% of total $\lambda_{du}$	Detection through
Z202, Z204, Z206, Z244, Z245, Z246, Z408, Z409, Z410, Z241, Z242, Z243	14,40%	100% functional test with different expected output signals
T505	6,55%	100% functional test with different expected output signals
T503-B	5,46%	100% functional test with different expected output signals
T202	5,46%	100% functional test with different expected output signals
IC501-B	5,24%	100% functional test with different expected output signals
C105, C106	4,36%	100% functional test with different expected output signals
T201	3,60%	100% functional test with different expected output signals
D102	3,49%	100% functional test with different expected output signals
C201	3,49%	100% functional test with different expected output signals
T503-A	3,27%	100% functional test with different expected output signals

### Appendix 1.1: Possible proof tests to detect dangerous undetected faults

A possible proof test is described in section 10 of the safety manual ([D5]) for the 9203 Solenoid / Alarm Driver.

## Appendix 2: Impact of lifetime of critical components on the failure rate

According to section 7.4.7.4 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.3) this only applies provided that the useful lifetime<sup>15</sup> of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolyte capacitors can be very sensitive).

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components. Therefore it is obvious that the  $PFD_{AVG}$  calculation is only valid for components which have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

It is assumed that early failures are detected to a huge percentage during the installation period and therefore the assumption of a constant failure rate during the useful lifetime is valid.

When plant experience indicates a shorter useful lifetime than indicated in this appendix, the number based on plant experience should be used.

---

<sup>15</sup> Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.

### Appendix 3: Description of the considered profiles

#### *exida* electronic database:

Profile	Profile according to IEC 60654-1	Ambient Temperature [°C]		Temperature Cycle [°C / 365 days]
		Average (external)	Mean (inside box)	
1	B2	30	60	5
2	C3	25	30	25
3	C3	25	45	25

#### PROFILE 1:

Cabinet mounted equipment typically has significant temperature rise due to power dissipation but is subjected to only minimal daily temperature swings.

#### PROFILE 2:

Low power electrical (two-wire) field products have minimal self heating and are subjected to daily temperature swings.

#### PROFILE 3:

General (four-wire) field products may have moderate self heating and are subjected to daily temperature swings.